Industrial Network Security

California Department of Transportation, District 2
Jeremiah Pearce, P.E. – ITS Engineer
Jeremiah.Pearce@dot.ca.gov

2017 Western States Rural Transportation Technology Implementers Forum – Yreka, CA
Industrial Network Security

• First What is an Industrial Network and what sets it apart from an administrative network?
  – Loosely defined an industrial network is a machine-to-machine, process control network environment
  – This is different from an administrative network which has many unique users running varying applications.

• Industrial Networking has been a growing market for years now

• Examples include, power plant, mining, rail, manufacturing, transportation management, etc.
Why do we need to worry about Network Security?
Administrative Network Hack
Example (Extreme)

Interaction varies

Target

Compromised machine results in stolen sensitive information

Attacker

Result
Why do we need to worry about Network Security?

What happens when an industrial network is not secure?
Industrial Network Hack

Example (Extreme)

Compromised machine
Results in loss of control

Target

Interaction varies

Attacker

Result

Chernobyl Disaster
Attacker

TMS Network Hack
Example Typical
TMS Network Hack Example (Extreme)

Interaction varies

Target

Compromised machine
Results in loss of control

Attacker

Result
How do these networks get compromised?

- Depends on a number of factors
  - Configuration
  - Physical security
  - Network topology
  - Or other methods

- There’s always a way in...
Industrial Network Security

• Recent Industrial Networking security issues
  – RUGGEDCOM authentication bypass issue - 2013
  – RUGGEDCOM switch VLAN routing feature - 2015
  – Moxa multiple vulnerabilities - 2016

• Industrial Network security is unique in two ways,
  – Culture. Products are specialized and don’t normally go through the same amount of scrutiny traditional IT hardware and software products experience
  – Industrial Network security objective prioritization
    • Availability
    • Integrity
    • Confidentiality
Industrial Network Security

- What do we do about security, how do we implement it?
  - First, define and prioritize your security objectives
  - Second, define your known vulnerabilities
  - Third, define what steps are being taken to mitigate the vulnerabilities (sometimes the vulnerability is an acceptable risk)

- This is known as a Security Policy and is a formal written document maintained by the network manager
Industrial Network Security

• Other issues to note...
• Balancing security with network availability and data integrity is the challenge with Industrial Networking
• Security feature availability is an issue with the industry
• After implementation there will likely be some risks, a tradeoff between implementation cost, the purpose of the network (what is it’s function – our network doesn’t have sensitive data so we don’t encrypt links), etc.
• Embedded Linux device security - Shell Shock, etc.
District 2 FEN Security

• Review of the District 2 Field Element Network (FEN)
  – “Field Element Network Design for a Rural Transportation Management Center, Parts One and Two” Ian Turnbull and Jeremiah Pearce, June 2012

http://www.westernstatesforum.org/Documents/2012/presentations/CaltransD2_Pearce_Final2_FEN_TMC_Part2.pdf
District 2 FEN Security

• Review of the District 2 Field Element Network (FEN)
  – “The Field Element Communications End Game - From POTS to Licensed Microwave” Jeremiah Pearce, June 2014
References


References


Questions